Aussies in lockdown

NortonLifeLock Digital Transformation Report 2020

83%* of Aussie respondents believe
cybercriminals have used COVID-19 to their advantage
As a result, Australians are more cautious of being affected by cybercrime

65% of respondents claim they have become more vigilant about their online security during lockdown

1 in 6
Aussie respondents were a victim of cybercrime during lockdown
Phishing email was the most common form of attack

37% of respondents noticed an increase in cybercrime activity during lockdown

(ie scams, phishing emails, fake shopping or charity sites)

87% of Aussie respondents feel they adapted well to the lockdown period

4 in 5 respondents
would consider working/studying from home on a more permanent basis

83% Gen X & Millennials	77% Gen Z
70% Boomers	84% NSW

62% of respondents
are using social media more

Since lockdown started,
21% of those surveyed have upgraded their existing software

55% of respondents have increased their usage of conferencing tools
(non-work related)

9% started purchasing essential items from unknown/ unfamiliar shopping sites since lockdown

81% of working respondents have used their personal device for work/study during lockdown

52% of respondents surveyed have paid cyber security software on their personal device/s
Of those surveyed only 44% of Gen Z have paid security software

42%
of respondents now participate in online gaming since lockdown

1 in 3 respondents have signed up to a subscription service since lockdown
(ie gaming, magazines, books, streaming services)

More than half of parents surveyed said
monitoring their child's online habits became more difficult
Though, 70% of these parents felt the transition to studying and learning from home was a great experience

60% were concerned about cyber risks

Boomers were the largest group to review privacy policies at 64%

10% more Aussie respondents now read privacy policies more closely since lockdown

18% of Millennials was the largest increase

74% of respondents are now paying for groceries or utility bills online with their credit/debit card

An increase of 12% pre-lockdown

44% are now using a digital wallet such as Apple Pay or Paypal when paying for their purchases

57% of respondents are doing more online shopping

Top tips to help you stay safe online

- Keep your VPN turned on. Unencrypted connections may give cyber criminals a chance to snoop on data being sent and received by your device
- Beware of COVID-19 themed phishing emails. Cybercriminals are exploiting the coronavirus outbreak to send fake emails with dangerous links to employees. Here's how it works. The email messages may appear to come from company officials and might ask you to open a link to a new company policy related to the coronavirus. If you click on the attachment or embedded link, you're likely to download malware onto your device. Don't click. Instead, immediately report the phishing attempt to your employer
- Manage your passwords. Use two-step or multi-factor authentication wherever offered to help prevent unauthorised access to your online accounts. Always change the default passwords regularly (every 3 months) to something strong and unique on your devices, services, and Wi-Fi networks
- Only use trusted sites when providing your personal information. A good rule of thumb is to check the URL. If the site includes "https://," then it's a secure site. If the URL includes "http://," — note the missing "s" — avoid entering sensitive information like your credit card data or tax file number
- Don't open email attachments or click links in emails from unknown sources. One of the most common ways networks and users are exposed to malware and viruses is through emails disguised as being sent by someone you trust
- Always keep your devices updated. Software updates contain important patches to fix security vulnerabilities. Cyber attackers can also target outdated devices which may not be running the most current security software
- Back up your files regularly for extra protection in the event of a cyber security attacks. If you need to wipe your device clean due to a cyberattack, it will help to have your files stored in a safe, separate place

*This survey was conducted online within Australia between July 14th – 20th 2020 among 1,000 adults. Figures for age, sex, race/ethnicity, education, region, employment, marital status, household size and household income were weighted where necessary to bring them into line with their actual proportions in the population. Propensity score weighting was used to adjust for respondents' propensity to be online.

NortonLifeLock™